Fordham Law Review

Volume 73 | Issue 5 Article 10

2005

Sliding Down a Slippery Slope? The Future Use of Administrative Subpoenas in Criminal Investigations

Risa Berkower

Sliding Down a Slippery Slope? The Future Use of Administrative Subpoenas in Criminal Investigations

Cover Page Footnote

J.D. Candidate, Fordham University School of Law. I would like to thank Professor Daniel Richman for his thoughtful advice and guidance with this Note. I am also grateful for the love, support, and encouragement of my parents, Jackie and Ira, my sisters, Ariel and Simone, and, of course, Sam.

NOTES

SLIDING DOWN A SLIPPERY SLOPE? THE FUTURE USE OF ADMINISTRATIVE SUBPOENAS IN CRIMINAL INVESTIGATIONS

*Risa Berkower**

INTRODUCTION

Consider the following hypothetical situation: FBI agents suspect that a local doctor is defrauding health insurance companies by over-billing them. Although the agents do not have probable cause to get a search warrant for the doctor's record room, they can use an administrative subpoena to mandate production of the doctor's records. If the records obtained by the subpoena reveal fraud, a United States Attorney can prosecute the doctor using this evidence.

In criminal proceedings, investigators' access to business records and other private documents is limited by the Fourth Amendment's search warrant requirement[1] and the Fifth Amendment's grand jury requirement.[2] However, as part of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), Congress delegated administrative subpoena power to the Attorney General to conduct criminal investigations into federal health care fraud.[3] Administrative subpoena power enables government investigators to bypass the Fourth Amendment's probable cause requirement to obtain private

---

* J.D. Candidate, 2006, Fordham University School of Law. I would like to thank Professor Daniel Richman for his thoughtful advice and guidance with this Note. I am also grateful for the love, support, and encouragement of my parents, Jackie and Ira, my sisters, Ariel and Simone, and, of course, Sam.

1. The Fourth Amendment provides:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

U.S. Const. amend. IV.

2. U.S. Const. amend. V ("No person shall be held to answer for a capital, or otherwise infamous crime, unless on a presentment or indictment of a Grand Jury . . . .").

3. Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), Pub. L. No. 104-191, § 248, 110 Stat. 1936, 2018 (codified at 18 U.S.C. § 3486 (2000)).

records.[4] Congress granted this power in reaction to public outcry against this increasingly prevalent crime and its effect on the rising cost of health care.[5] In a May 2002 report to Congress, the Department of Justice's Office of Legal Policy found that Congress had granted health care fraud investigators a highly effective investigatory tool. Administrative subpoenas proved extremely useful to both investigators and prosecutors because, unlike traditional investigatory tools, the subpoenas enabled law enforcement agents acting on mere suspicion to access private information and placed few prohibitions on the use of that information.[6]

Consider a second hypothetical situation: FBI agents suspect that an al-Qaeda sleeper cell may be planning a chemical attack in a particular city. The agents want to obtain all sales records from hardware stores in the area to see if any large chemical purchases were recently made. However, since the agents do not have probable cause to get a search warrant, they cannot pursue this lead.

The success with which federal agents and prosecutors have used the HIPAA administrative subpoenas raises the question of whether this power should be expanded to other types of criminal investigations.[7] Since the September 11, 2001 terrorist attacks, the federal government has pushed to make terrorism investigations easier and more effective.[8] One proposal would grant the FBI administrative subpoena power to obtain easier access to business records and other private documents in terrorism investigations,[9] such as in the second hypothetical above. However, administrative subpoena power is useful in a criminal investigation primarily because it enables investigators to bypass the Fourth Amendment's probable

4. United States v. Powell, 379 U.S. 48, 57 (1964) (rejecting probable cause as the standard governing Internal Revenue Service administrative subpoenas); *see* SEC v. Jerry T. O'Brien, Inc., 467 U.S. 735, 741-42 (1984) (holding that the standards set in *Powell* govern all administrative subpoenas).

5. *See* H.R. Rep. No. 104-496, at 66-69 (1996), *reprinted in* 1996 U.S.C.C.A.N. 1865, 1866-68.

6. *See* Office of Legal Policy, U.S. Dep't of Justice, Report to Congress on the Use of Administrative Subpoena Authorities by Executive Branch Agencies and Entities 35 (2002) [hereinafter DOJ Report], *available at* http://www.justice.gov/olp/intro.pdf. The report, required by the Presidential Threat Protection Act of 2000, Pub. L. No. 106-544, § 7, 114 Stat. 2715, 2719, found that in 2001 federal prosecutors issued 2102 administrative subpoenas for health care fraud investigations. *See* DOJ Report, *supra*, at 40-41 tbl. 1.

7. *See* Republican Policy Comm., Updating the Law to Confront New Challenges: Should Postal Inspectors Have More Power than Federal Terrorism Investigators? [hereinafter Updating the Law], *available at* http://rpc.senate.gov/_files/Sept0904JetsSDAH.pdf (last visited Feb. 17, 2005).

8. *See* Alfred Cumming & Todd Masse, Congressional Research Service, FBI Intelligence Reform Since September 11, 2001: Issues and Options for Congress 1, 4 (Apr. 6, 2004) [hereinafter FBI Intelligence Reform], *available at* http://fpc.state.gov/documents/organization/32038.pdf.

9. *See* S. 2555, 108th Cong. (2004); H.R. 3037, 108th Cong. (2003).

cause requirement for criminal investigations[10]—a requirement that protects not only criminal suspects' privacy rights, but also the rights of innocent individuals from unreasonable government intrusions. Because of this, using administrative subpoenas in broad terrorism investigations would implicate Fourth Amendment rights on a grand scale.

Since the social costs of terrorism are infinitely higher than that of health care fraud, if constitutional criminal procedures can be compromised to combat health care fraud it might make sense to do the same for fighting terrorism. As President George W. Bush stated, "'[i]f we can use these [administrative] subpoenas to catch crooked doctors . . . the Congress should allow law enforcement officials to use them in catching terrorists.'"[11] However, this reasoning could also create a slippery slope of exceptions and allowances to traditional criminal processes that would ultimately erode the constitutional safeguards built into all criminal investigations.

This Note addresses the Fourth Amendment implications of giving administrative subpoena power to the FBI for use in criminal investigations. Part I.A explains the probable cause requirement and how investigators use the traditional criminal processes of search warrants and grand jury subpoenas to obtain private information. Part I.B compares these criminal processes to the development of administrative investigatory subpoenas. Part I.C discusses the modern-day intersection of civil and criminal investigative processes, the federal judiciary's reaction to this, and the current limitations on the use of administrative subpoena power in criminal investigations. Part I.D follows by detailing why proposals to grant administrative subpoena power to the FBI for terrorism investigations were introduced in both houses of Congress.

Parts II.A and II.B explain the arguments for and against giving the FBI administrative subpoena power for terrorism investigations in light of the implications for Fourth Amendment rights.

Finally, Part III concludes that terrorism administrative subpoenas would seriously undermine Fourth Amendment privacy rights. Part III.A argues that the justifications for abrogating Fourth Amendment rights in health care fraud investigations are neither analogous nor compelling for terrorism and other criminal investigations. Part III.B contends that terrorism administrative subpoenas would carry significant secondary implications for Fourth Amendment rights even if persuasive reasons justify granting the FBI this subpoena power. In

10. *See* Doe v. United States, 253 F.3d 256, 263 (6th Cir. 2001) (finding that no probable cause is required to issue an administrative subpoena under Section 248 of HIPAA); United States v. Bailey, 228 F.3d 341, 348 (4th Cir. 2000) (same).

11. *See* David E. Sanger, *President Urging Wider U.S. Powers in Terrorism Law*, N.Y. Times, Sept. 11, 2003, at A1 (quoting President Bush's Sept. 10, 2002 address at the FBI training academy in Quantico, Virginia).

the alternative, Part III.C recommends measures that Congress should take to prevent damage to individuals' Fourth Amendment rights in other criminal investigations.

I. BACKGROUND AND HISTORY OF GOVERNMENTAL TOOLS TO OBTAIN PRIVATE INFORMATION

This part describes the history of civil and criminal investigatory tools, and how civil subpoenas first came to be used in criminal investigations. Part I.A provides background information on traditional criminal investigatory tools. Part I.B explains the development of civil subpoena power. Part I.C discusses the first congressional provision for civil subpoena power in a criminal investigation and the federal appellate opinions addressing that provision. Finally, Part I.D introduces the current debate regarding the use of administrative subpoenas in terrorism investigations.

A. *Traditional Criminal Procedures to Obtain Private Information*

Traditionally, information gathering for criminal investigations requires that law enforcement officers have a search warrant or a grand jury subpoena.[12]

1. Search Warrants and the Probable Cause Requirement

Interpreting the Fourth Amendment's prohibition against unreasonable searches and seizures, the Supreme Court requires that law enforcement officers conduct all searches and seizures pursuant to a valid search warrant that is supported by probable cause.[13] The probable cause requirement means that before law enforcement officers can invade an individual's privacy, they must have some evidence that the search will reveal criminal activity.[14] The probable cause requirement exists to protect all individuals and their possessions from indiscriminate government searches and seizures,[15] and it "has roots that are deep in our [nation's] history."[16] The framers of the Fourth Amendment included the probable cause requirement in reaction to the arbitrary abuses of police power suffered under the British Crown.[17] By preventing unjustified, excessive state searches, the probable cause requirement protects

12. *See* U.S. Const. amends. IV-V.

13. 2 Wayne R. LaFave, Search and Seizure: A Treatise on the Fourth Amendment § 4.1, at 441 (4th ed. 2004).

14. *See* Ronald M. Gould & Simon Stern, *Catastrophic Threats and the Fourth Amendment*, 77 S. Cal. L. Rev. 777, 786 (2004).

15. Anthony G. Amsterdam, *Perspectives on the Fourth Amendment*, 58 Minn. L. Rev. 349, 411 (1974).

16. Henry v. United States, 361 U.S. 98, 100 (1959).

17. *See* Gould & Stern, *supra* note 14, at 791-92.

innocent individuals from baseless searches[18] and legitimizes the governmental intrusions of privacy that do take place.[19]

Aside from a few carefully defined exceptions, "a search of private property without proper consent [violates the Fourth Amendment] unless it has been authorized by a valid search warrant [that is supported by probable cause]."[20] A search warrant "is a judicial authorization to a law enforcement officer to search or seize persons or things."[21] To obtain a search warrant, a law enforcement officer must prove to a judge that there is probable cause to support the warrant.[22] Search warrants "serve[] a high function"[23] because the right to be "free from unreasonable governmental intrusion [stands] at the very core of the Fourth Amendment."[24]

The search warrant requirement recognizes that neutral magistrates uninvolved with an investigation can make a better decision as to whether probable cause justifies a search than law enforcement officers "'engaged in the often competitive enterprise of ferreting out crime.'"[25] Physical searches can be an immediate and substantial privacy intrusion.[26] By requiring that only neutral judicial officers can issue search warrants upon a demonstration of probable cause, the Fourth Amendment places an important checkpoint for judicial supervision between the government and the people.[27]

Search warrants, however, are not always the most effective investigative tool. Because of the probable cause requirement, investigators cannot use search warrants in cases of mere suspicion.[28] Also, since search warrants are issued without prior notice,[29] can be

18. *See* Sherry F. Colb, *Innocence, Privacy, and Targeting in Fourth Amendment Jurisprudence*, 96 Colum. L. Rev. 1456, 1464 (1996).

19. *See* Groh v. Ramirez, 540 U.S. 551, 561-62 (2004); Illinois v. Gates, 462 U.S. 213, 236 (1983) ("[P]ossession of a warrant by officers conducting an arrest or search greatly reduces the perception of unlawful or intrusive police conduct."); United States v. Chadwick, 433 U.S. 1, 9 (1977) (noting that a warrant "assures the individual whose property is searched or seized of the lawful authority of the executing officer, his need to search, and the limits of his power to search"); Stephen A. Saltzburg & Daniel J. Capra, American Criminal Procedure: Cases and Commentary 89-90 (7th ed. 2004).

20. *Groh*, 540 U.S. at 560 (quoting Camara v. Mun. Court, 387 U.S. 523, 528-29 (1967)).

21. United States v. Bailey, 228 F.3d 341, 348 (4th Cir. 2000).

22. *See* Saltzburg & Capra, *supra* note 19, at 91.

23. *Groh*, 540 U.S. at 557 (quoting McDonald v. United States, 335 U.S. 451, 455 (1948)).

24. *Id.* (quoting Kyello v. United States, 533 U.S. 27, 31 (2001) (internal quotations omitted)).

25. 2 LaFave, *supra* note 13, § 4.1(a), at 442 (quoting Johnson v. United States, 333 U.S. 10, 14 (1948)).

26. *Bailey*, 228 F.3d at 348.

27. *Id.* (citing Steagald v. United States, 451 U.S. 204, 212 (1981)).

28. Graham Hughes, *Administrative Subpoenas and the Grand Jury: Converging Streams of Criminal and Civil Compulsory Process*, 47 Vand. L. Rev. 573, 575 (1994).

29. *See Bailey*, 228 F.3d at 348.

executed immediately,[30] and are often executed with force constituting an "unanticipated physical intrusion,"[31] warrants may be an unnecessarily harsh and intrusive means of obtaining information from third parties who might be willing to surrender information on demand.[32] Recognizing this, the United States Attorney's Criminal Resource Manual counsels that warrants should not be used in a criminal investigation if the information sought can be obtained through other less intrusive means.[33] Finally, warrants can only authorize the seizure of goods, effects, and papers—they cannot be used to compel testimony.[34]

Although search warrants authorize potentially invasive searches and seizures, warrants can only be challenged after execution by a motion to suppress any evidence obtained in the search, on the grounds that the search was unreasonable.[35] The challenging party usually bears the burden of proving that a search executed with a warrant was unreasonable because district courts give deference to the neutral judicial officer's finding of probable cause for the search.[36] However, third parties lack standing to challenge the validity of a search that may affect the third party's privacy interests, such as the search of a business premises that contained the party's private records.[37]

---

30. *See* 2 LaFave, *supra* note 13, § 4.7, at 645-60. Although notice is required, the notice can be given immediately before the warrant is executed. *See* 2 *id.* § 4.8, at 660-702.

31. *Bailey*, 228 F.3d at 348 (citing Marshall v. Barlow's Inc., 436 U.S. 307, 316 (1978)).

32. Hughes, *supra* note 28, at 575.

33. Specifically, warrants are only authorized if reliance on alternative means would "substantially jeopardize [the] availability . . . or usefulness [of the information]." Dept. of Justice, United States Attorney's Manual, 28 C.F.R. § 59.1 (2005). Title II of the Privacy Protection Act of 1980 requires the Attorney General to

> issue guidelines for the procedures to be employed by any Federal officer or employee, in connection with the investigation or prosecution of an offense, to obtain documentary materials in the private possession of a person when the person is not reasonably believed to be a suspect in such offense . . . and when the materials sought are not contraband or the fruits or instrumentalities of an offense.

42 U.S.C. § 2000aa-11 (2000).

34. Hughes, *supra* note 28, at 575.

35. 2 LaFave, *supra* note 13, § 4.1f, at 471-75.

36. 6 *id.* § 11.2b, at 43-44.

37. 6 *id.* § 11.3d, at 190-91 (citing United States v. Miller, 425 U.S. 435 (1976) (seizure of bank records cannot be challenged by customer)); *see also* United States v. Plunk, 153 F.3d 1011, 1019-20 (9th Cir. 1998) (phone records seized from phone company could not be challenged by customer).

2. Grand Jury Subpoenas

Law enforcement agents and prosecutors can also access private information by grand jury subpoenas.[38] Grand juries serve both an indicting and an investigatory function.[39] As a consequence, a grand jury may uncover evidence that leads to formal criminal charges, but its investigation may also clear innocent suspects.[40] Ordinarily, grand juries screen prosecutors' cases to determine whether the prosecutor has enough evidence against a suspect to support criminal charges.[41] During an investigation into a crime, the grand jury possesses the broadest subpoena power known in law to compel witness testimony or to produce evidence.[42] Failure to comply with a grand jury subpoena is punishable by civil or criminal contempt.[43]

The standards for issuing a grand jury subpoena are lower than for issuing a search warrant,[44] and the grand jury's investigation is afforded broad scope.[45] Whereas law enforcement officers must have probable cause to get a search warrant, and warrants must specify the location to be searched and the items to be seized,[46] grand juries can investigate "merely on suspicion that the law is being violated, or even just because it wants assurance that it is not."[47] To fulfill this investigatory mission, grand juries must "paint[] with a broad brush," until "'every available clue has been run down and all witnesses examined in every proper way to find if a crime has been committed.'"[48] Because of this, grand jury investigations can be especially effective to investigate crimes with no identifiable victim.[49]

---

38. 1 Sara Sun Beale et al., Grand Jury Law and Practice § 1:7, at 1-32 to 1-33 (2d ed. 2001).

39. 1 *Id.* at 1-31; *see* Daniel C. Richman, *Grand Jury Secrecy: Plugging the Leaks in an Empty Bucket*, 36 Am. Crim. L. Rev. 339, 342-45 (1999) [hereinafter Richman, *Grand Jury Secrecy*].

40. *See* 1 Beale et al., *supra* note 38, § 1:7, at 1-31 to 1-32.

41. 1 *id.* This function of the grand jury is frequently and harshly criticized in the academic literature as a farce in which the grand jury acts as a rubber stamp for prosecutors—the often quoted accusation is that "a Grand Jury would indict a 'ham sandwich.'" *In re* Grand Jury Subpoena of Stewart, 545 N.Y.S.2d 974, 977 n.1 (App. Div. 1989) (quoting the Chief Justice of the New York Court of Appeals's publicly stated skepticism about grand juries). For an interesting discussion about the role of grand juries in the modern federal criminal justice system, see generally Niki Kuckes, *The Useful, Dangerous Fiction of Grand Jury Independence*, 41 Am. Crim. L. Rev. 1 (2004).

42. 1 Beale et al., *supra* note 38, § 1:7, at 1-32 to 1-33, § 5:1, at 5-5.

43. 1 *id.* § 6:1, at 6-4.

44. 1 *id.* § 6:3, at 6-19 (no probable cause required).

45. *See* United States v. Dionisio, 410 U.S. 1, 15 (1973).

46. U.S. Const. amend. IV.

47. United States v. Morton Salt Co., 338 U.S. 632, 642-43 (1950).

48. United States v. R. Enters., Inc., 498 U.S. 292, 297 (1991) (quoting Branzburg v. Hayes, 408 U.S. 665, 701 (1972)).

49. 1 Beale et al., *supra* note 38, § 1:7, at 1-33. Examples include business crime, political corruption, and organized crime where witnesses often are also participants in the crime. 1 *id.* § 6:1, at 6-4.

Grand jury subpoenas also enable third parties, such as a bank or other business, to give up private information about criminal suspects without risk.[50] A subpoena's legal force enables a third party to explain its cooperation with authorities as required by law, and not a desire to "turn in" a customer, despite authorities' lack of probable cause.[51] Although the prosecutor, and not the grand jury itself, decides what witnesses and evidence to subpoena,[52] a prosecutor can only issue subpoenas to further the grand jury's investigation of a crime.[53] However, the technical procedural and evidentiary rules that govern criminal trials do not constrain grand juries; grand juries may compel the production of evidence as they consider appropriate.[54]

The grand jury's extensive power is subject to two important limitations. First, the grand jury can only investigate criminal matters, and all grand jury proceedings are secret pursuant to the Federal Rules of Criminal Procedure.[55] Second, the grand jury cannot compel testimony or demand physical evidence for any purpose other than a criminal investigation.[56] This limitation recognizes a compromise between the public interest in investigating crimes and limiting intrusions to privacy—since the public interest is higher in solving crime than in investigating civil matters, broader investigatory techniques are acceptable for criminal cases but not for civil cases.[57]

Additionally, a complex set of rules keep grand jury proceedings secret, albeit with important exceptions.[58] The Supreme Court identified five justifications for grand jury secrecy that the Court still accepts: (1) to prevent criminal suspects from fleeing; (2) to ensure that the grand jury can deliberate freely, without pressure from interested parties; (3) to prevent witness tampering or subornation of perjury; (4) to encourage witnesses to testify fully and honestly; and (5) to protect the privacy of accused parties who are ultimately

---

50. 1 *id.* § 6:1, at 6-7.

51. *Id.*

52. Prosecutors often make these decisions independently because they can require technical knowledge of the law. 1 *id.* § 6:2, at 6-12; *see also* Andrew D. Leipold, *Why Grand Juries Do Not (and Cannot) Protect the Accused*, 80 Cornell L. Rev. 260, 315-16 (1995).

53. 1 Beale et al., *supra* note 38, § 6:2, at 6-12 to 6-14 (subpoenas not issued to further the grand jury's investigation into a crime are an abuse of the grand jury's subpoena authority).

54. United States v. R. Enters., Inc., 498 U.S. 292, 298 (1991).

55. Fed. R. Crim. P. 6(e) (rule governing the recording of grand jury proceedings, the secrecy of the proceedings, and the limited exceptions to the secrecy requirement); *see* Hughes, *supra* note 28, at 577 (describing the limitations on the use of grand jury information).

56. *See* Hughes, *supra* note 28, at 611 n.149 (discussing Federal Rule of Criminal Procedure 6(e)(3)(b)). The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001 changed this rule in certain circumstances. *See infra* note 111.

57. *See* Hughes, *supra* note 28, at 577, 633.

58. *See* 1 Beale et al., *supra* note 38, § 5.

exonerated.[59] While grand jury secrecy on its own may not wholly address these concerns,[60] the secrecy requirement arguably provides important protection to witnesses compelled to testify or reveal sensitive documents without the safeguards of an attorney, the relevancy limits of trial, or the privilege against self-incrimination.[61] Although critics debate the importance and efficacy of grand jury secrecy in the larger context of criminal investigations,[62] traditionally the secrecy requirement is viewed as a recognition that the grand jury's unparalleled investigatory powers can be justified only to help the government reach the point of charging a suspect with a crime.[63]

Subpoena recipients can challenge the demand before complying with it, but winning a motion to quash is extremely difficult. Under Rule 17(c)(2) of the Federal Rules of Criminal Procedure, grand jury subpoenas cannot be "unreasonable or oppressive."[64] However, because grand jury investigations must be broad, grand jury subpoenas bear a presumption of reasonableness.[65] Considering a motion to quash requires the court to balance the government's interest in obtaining the information demanded and the burden of the subpoena's demands on the recipient.[66] Any challenger bears either the difficult burden of proving that "there is no reasonable possibility that the category of materials the Government seeks will produce information relevant to the general subject of the grand jury's investigation," or that compliance with the subpoena would be unreasonably burdensome.[67] To slightly alleviate these seemingly impossible burdens of proof, the subject of the grand jury's investigation, usually covered by the secrecy requirement, can be revealed to a subpoena's challenger.[68] However, because of the high

59. Douglas Oil, Co. v. Petrol Oil Stops Northwest, 441 U.S. 211, 219 n.10 (1979); *see also* Richman, *Grand Jury Secrecy*, *supra* note 39, at 352-53 (discussing *Douglas Oil*).

60. Richman, *Grand Jury Secrecy*, *supra* note 39, at 353 (arguing that these concerns justify overall investigative secrecy, not just grand jury secrecy).

61. *Id.* at 354 (noting that the secrecy requirement protects grand jury witnesses who may be more vulnerable to injury and so more deserving of protection because they must testify without the protections available to witnesses in other circumstances, such as at trial).

62. *See* Hughes, *supra* note 28, at 635-40; Richman, *Grand Jury Secrecy*, *supra* note 39, at 352-56.

63. *See* Hughes, *supra* note 28, at 667-68. *See generally* Leipold, *supra* note 52, at 265-68 (discussing grand jury secrecy).

64. Fed. R. Crim. P. 17(c)(2); *see* 1 Beale et al., *supra* note 38, § 6:21, at 6-185 (discussing the reasonableness requirement for grand jury subpoenas).

65. 1 Beale et al., *supra* note 38, § 6:21, at 6-186 (citing United States v. R. Enters., Inc., 498 U.S. 292 (1991)).

66. *See R. Enters.*, 498 U.S. at 300.

67. *Id.* at 301.

68. 1 Beale et al., *supra* note 38, § 6:21, at 6-186 (discussing *R. Enters.*). In a sensitive investigation, the subject could be revealed to the court in camera so that the judge could determine whether a motion to quash the subpoena had a reasonable chance of success. *Id.*

burdens of proof imposed on a challenger, most grand jury subpoenas will ultimately be enforced. Also, because an adverse ruling on a motion to quash a subpoena is not an appealable final order, the likelihood that a subpoena recipient will be able to avoid compliance is further limited.[69]

B. *Development of Administrative Agencies' Investigative Power*

Information gathering tools for civil administrative agency investigations developed differently from those used in criminal investigations. Congress enables administrative agencies to enforce their regulations by delegating subpoena power to them.[70] Administrative subpoenas can demand records and require witnesses to testify about the records' accuracy.[71] The Supreme Court construes administrative agencies' subpoena power broadly—a civil subpoena will be enforced so long as the "evidence sought . . . [is] not plainly incompetent or irrelevant to any lawful purpose."[72] Like the grand jury, an agency need not show probable cause to issue a subpoena; a court must only find that "the inquiry is within the authority of the agency, the demand is not too indefinite and the information sought is reasonably relevant [to the inquiry]."[73] Even subpoenas that are "fishing expeditions" are valid so long as they seek to ensure compliance with the agency's regulations.[74]

The Court's jurisprudence supports this broad subpoena authority with three main justifications. First, broad administrative subpoena power is necessary because it enables Congress to delegate power to administrative agencies to investigate violations of federal law.[75] In this regard, administrative agency investigations serve the same function as a grand jury investigation.[76] Additionally, as with a grand jury's subpoena,[77] administrative subpoenas cannot be arbitrary and

---

69. *See* Hughes, *supra* note 28, at 595.

70. *See* Kenneth F. Warren, Administrative Law in the Political System 527 (4th ed. 2004). Congress started to grant agencies these powers during the New Deal and World War II, as the regulatory role of administrative agencies, and hence agencies' need for information from regulated entities, expanded. *See* Kenneth Culp Davis & Richard J. Pierce, Jr., Administrative Law Treatise § 4.1, at 138 (3d ed. 1994). For a history of the development of administrative subpoena power, see Katherine Scherb, Comment, *Administrative Subpoenas for Private Financial Records: What Protection for Privacy Does the Fourth Amendment Afford?*, 1996 Wis. L. Rev 1075, 1076-85.

71. *See* Cudahy Packing Co. v. Holland, 315 U.S. 357, 363 (1942) (recognizing that administrative subpoena power can be used coercively).

72. Endicott Johnson Corp. v. Perkins, 317 U.S. 501, 509 (1943); *see also* United States v. LaSalle Nat'l Bank, 437 U.S. 298 (1978); United States v. Powell, 379 U.S. 48, 57 (1964).

73. United States v. Morton Salt Co., 338 U.S. 632, 642-43, 652 (1950).

74. Hughes, *supra* note 28, at 588-89 (discussing the effects of *Morton Salt*).

75. Okla. Press Publ'g Co. v. Walling, 327 U.S. 186, 201 (1946).

76. *Id.* at 216.

77. *See supra* notes 38-69 and accompanying text (discussing grand jury subpoenas).

the agency cannot act outside its statutory authority,[78] but "this does not mean that [the agency's] inquiry must be 'limited narrowly by . . . forecasts of the probable result of the investigation.'"[79] Instead, as in a grand jury investigation, an agency issues an administrative subpoena to "discover and procure evidence, not to prove a pending charge."[80] Without subpoena power similar to that of a grand jury, administrative agencies could not effectively investigate alleged violations of the laws and regulations that the agency is charged with enforcing.[81]

Second, broad administrative agency subpoena power does not infringe upon Fourth Amendment privacy rights because the Court treats civil and criminal cases differently for Fourth Amendment purposes.[82] Administrative agency subpoenas need only meet a reasonableness standard, not a stricter probable cause standard, to comply with the Fourth Amendment.[83] This lower standard is appropriate because, for many regulations, the only evidence of a violation will exist in a company's records.[84] As a result, if agencies had to meet a strict probable cause standard to obtain access to such records, agencies could not effectively enforce their regulations.[85]

In assessing an administrative subpoena's reasonableness under the Fourth Amendment, the Court uses a four-factor test: (1) whether the investigation is conducted pursuant to a legitimate purpose; (2) whether the information requested by the subpoena is relevant to this purpose; (3) whether the information sought is already within the agency's possession; and (4) whether the agency followed all statutory requirements in issuing the subpoena.[86] The Court must make an individualized inquiry into the context of the subpoena, because factors like the relevancy of the requested information and the adequacy or excess of the subpoena's breadth vary with the nature, purpose, and scope of the issuing agency's inquiry.[87] However, since an administrative subpoena need not meet a stringent probable cause

78. *Okla. Press*, 327 U.S. at 216.

79. *Id.* (quoting Blair v. United States, 250 U.S. 273, 282 (1919)).

80. *Id.* at 201.

81. *See* DOJ Report, *supra* note 6, at 7 & n.9.

82. *See* Warren, *supra* note 70, at 520; Ronald F. Wright, Note, *The Civil and Criminal Methodologies of the Fourth Amendment*, 93 Yale L.J. 1127, 1127 (1984).

83. *See* United States v. Powell, 379 U.S. 48, 51 (1964). This was not always the case. The Court originally demanded that agencies meet a probable cause standard to demand records for regulatory purposes. *See* FTC v. Am. Tobacco Co., 264 U.S. 298, 305-06 (1924) (condemning "fishing expeditions" in agency investigations). The Court reversed this position in 1943, reflecting a recognition of administrative agencies' growing social importance during the New Deal and World War II. *See* Endicott Johnson Corp. v. Perkins, 317 U.S. 501, 509 (1943).

84. *See* Ernest Gellhorn & Ronald M. Levin, Administrative Law and Process 130 (4th ed. 1997).

85. *Id.*

86. *See Powell*, 379 U.S. at 57-58.

87. *See* Okla. Press Publ'g Co. v. Walling, 327 U.S. 186, 209 (1946).

standard to satisfy Fourth Amendment requirements against unreasonable searches and seizures,[88] the district court's review focuses on "insur[ing] the integrity" of the agency's investigative demands.[89]

Third, although agencies do not need probable cause to issue a subpoena, judicial review prevents agencies from abusing their subpoena power.[90] Unlike a search warrant, which is issued without prior notice and often executed with an unexpected physical intrusion,[91] an administrative subpoena "commences an adversar[ial] process"[92] that permits judicial review of the subpoena's reasonableness before the subpoenaed party is punished for noncompliance.[93] If a subpoenaed party challenges the demand as an unreasonable invasion of privacy rights, the district court must employ the four-factor reasonableness test established in *United States v. Powell* to evaluate the recipient's challenge.[94] Additionally, administrative agencies lack enforcement power—only federal courts, and not the agencies themselves, can enforce administrative subpoenas.[95] In an administrative investigation, if a subpoenaed party refuses to comply with the subpoena, the agency must go to a federal district court for an order of enforcement.[96] If the district court orders the subpoena's enforcement but the recipient still refuses to comply, the court can impose contempt sanctions.[97] However, judicial review provides an important check on administrative agencies that prevents

88. *See Powell*, 379 U.S. at 51.

89. Wearly v. FTC, 616 F.2d 662, 665 (3d Cir. 1980).

90. DOJ Report, *supra* note 6, at 9; *see also* United States v. Sec. State Bank and Trust, 473 F.2d 638, 641 (5th Cir. 1973).

91. *See supra* notes 29-34 and accompanying text.

92. United States v. Bailey, 228 F.3d 341, 348 (4th Cir. 2000).

93. *Id.* (quoting See v. City of Seattle, 387 U.S. 541, 544-45 (1967)).

94. 379 U.S. 48 (1964); *see* United States v. Morton Salt Co., 338 U.S. 632, 652-53 (1950) (holding that the agency request must be reasonable). Even if the subpoena meets the four-factor test's initial criteria to be enforceable, a recipient can challenge a subpoena on other substantive grounds such as improper purpose, that the subpoena demands privileged information, or that the subpoena infringes rights like the free exercise of religion, freedom of association, and the privilege against self-incrimination. *See* Doe v. Ashcroft, 334 F. Supp. 2d 471, 485 (S.D.N.Y. 2004); DOJ Report, *supra* note 6, at 9.

95. Some statutes require the agency to request that the U.S. Attorney's office seek enforcement of the subpoena in federal court instead of permitting the agency to seek enforcement on its own. DOJ Report, *supra* note 6, at 9-10.

96. *Id.* at 9 & n.20. However, some agencies take other action to push the subpoena recipients to "voluntarily" comply. *See id.* at 14. Additionally, some statutes granting agencies' subpoena power require the agency to ask the United States Attorney's office to seek enforcement. *Id.* at 9-10.

97. *Id.* at 11.

the enforcement of overreaching and unreasonable investigative demands.[98]

Several factors differentiate administrative subpoenas from criminal investigatory tools. First, as discussed above, unlike search warrants, administrative subpoenas do not require probable cause—administrative subpoenas need only be reasonable to satisfy the Fourth Amendment.[99] Also, in contrast to a search warrant, an administrative subpoena's compliance with the Fourth Amendment can be litigated before any privacy intrusion occurs.[100] Second, unlike grand jury subpoena recipients, administrative subpoena recipients receive extra protection from appellate review because a district court's denial of a motion to quash or modify the subpoena is an appealable final order.[101] Although most administrative subpoenas will be enforced because the Fourth Amendment reasonableness standard is difficult for a challenger to overcome,[102] this review process is a vital source of administrative subpoenas' legitimacy.[103] Finally, administrative agency investigations are not subject to the

98. *See* United States v. Bailey, 228 F.3d 341, 348 (4th Cir. 2000) ("As judicial process is afforded before any intrusion occurs, the proposed intrusion is regulated by, and its justification derives from, that process.").

99. *Compare supra* notes 13-37 and accompanying text, *with supra* notes 86-89 and accompanying text.

100. *See supra* notes 90-97 and accompanying text.

101. Cobbledick v. United States, 309 U.S. 323, 330 (1940) (holding that parties may immediately appeal district court orders enforcing these administrative subpoenas because administrative subpoenas are "self-contained, so far as the judiciary is concerned"); *see* Hughes, *supra* note 28, at 595. This stands in contrast to the denial of a motion to quash a grand jury subpoena, which cannot be appealed as a final order. *See supra* note 69 and accompanying text.

102. Although much of the subpoenas' legitimacy comes from the judicial review available to subpoenaed parties before they must comply with the demand, circuit courts describe the standards of review as "minimal" and the Supreme Court declared that, generally, courts must enforce an agency's subpoena unless the information demanded is "'plainly . . . irrelevant to any lawful purpose of the [agency].'" Doe v. Ashcroft, 334 F. Supp. 2d 471, 485 n.48 (S.D.N.Y. 2004) (quoting Endicott Johnson Corp. v. Perkins, 317 U.S. 501, 509 (1943)).

103. Doe v. United States, 253 F.3d 256, 264 (6th Cir. 2001) (noting that unlike a search warrant, "the reasonableness of an administrative subpoena's command can be contested in federal court before being enforced"); *Bailey*, 228 F.3d at 348. The *Bailey* court pointed out that

> [a]s judicial process is afforded before any intrusion occurs, the proposed intrusion is regulated by, and its justification derives from, that process. In short, the immediacy and intrusiveness of a search and seizure conducted pursuant to a warrant demand the safeguard of demonstrating probable cause to a neutral judicial officer before the warrant issues, whereas the issuance of [an administrative] subpoena initiates an adversary process that can command the production of documents and things only after judicial process is afforded.

Id.

strict secrecy requirements associated with grand jury proceedings.[104] As a result, information obtained by an administrative subpoena can be shared between government agencies.[105]

C. *Criminal and Civil Investigations Intersect*

Although civil and criminal investigative processes developed separately, in the context of administrative agency proceedings civil and criminal investigations overlap with ever-increasing frequency.[106] Since Congress often provides for both civil and criminal penalties for breaches of federal agencies' regulations,[107] to enforce its regulations an agency can often choose either to pursue civil penalties and administrative sanctions or recommend the case to the Department of Justice for prosecution.[108] One regulatory breach can, however, lead to parallel civil and criminal investigations and legal processes.[109] Because of this, the extent to which civil and criminal investigators can share findings becomes relevant. Grand jury subpoenas and administrative subpoenas both can demand a broad range of information.[110] However, information sharing between simultaneous administrative agency and grand jury investigations would necessarily be unbalanced, because while information obtained by an administrative subpoena could be shared with prosecutors and used in a criminal investigation, grand jury secrecy would prevent information from moving in the other direction.[111] This means that the

104. *See* Hughes, *supra* note 28, at 600-01 (noting that the information obtained by administrative subpoenas is to some degree confidential but is not subject to the strict secrecy requirement for grand jury subpoenas).

105. *See id.* (noting that unlike "the formidable barriers erected to prevent the disclosure of grand jury information," information obtained by administrative subpoenas can be "disclos[ed] in the public interest and without the necessity for a court order").

106. *Id.* at 578-80.

107. *Id.; see* Kenneth Mann, *Punitive Civil Sanctions: The Middleground Between Criminal and Civil Law*, 101 Yale L.J. 1795, 1801-02 (1992).

108. Hughes, *supra* note 28, at 578-89.

109. *Id.* at 586. Hughes also points out that a civil remedy may be more attractive because the burden of proof in civil proceedings is lower, discovery rules are more favorable, and the party may submit to a penalty rather than contest a criminal charge. *Id.* at 579.

110. *See supra* Part I.A.

111. *See* Hughes, *supra* note 28, at 593-94, 600-01. However, the PATRIOT Act further blurred the line between civil and criminal processes by creating an exception to Federal Rule of Criminal Procedure 6(e), which establishes grand jury secrecy. Under section 203 of the PATRIOT Act, prosecutors can disclose grand jury information involving foreign intelligence or counter-intelligence information to any federal law enforcement, intelligence, protective, immigration, national defense, or national security official. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001, Pub. L. No. 107-56, § 203(a), 115 Stat. 272, 278-80 (2001) (to be codified in scattered sections of 18 U.S.C.). For a thorough discussion of the PATRIOT Act's changes to Federal Rule of Criminal Procedure 6(e), see Jennifer M. Collins, *And the Walls Came Tumbling Down: Sharing Grand Jury Information with*

information obtained by an agency's civil subpoenas could end up in a prosecutor's office as the basis for a criminal prosecution—an agency's broad subpoena power could wholly undercut the grand jury's traditional function with fewer strings attached for prosecutors.[112] Since agency investigations are not subject to the secrecy requirement for grand jury investigations, and because administrative subpoenas do not require probable cause, the extent to which prosecutors can use the information gathered by an administrative subpoena carries serious implications for the privacy rights of individuals under investigation.

1. Using Civil Subpoenas for Criminal Law Enforcement Purposes: Section 248 of HIPAA[113]

In 1996, as part of HIPAA, Congress further entangled civil and criminal investigatory processes by granting the Attorney General the power to issue administrative subpoenas for use by the FBI in federal health care fraud investigations.[114] This bill marked the first time that Congress granted this broad investigative subpoena power solely for criminal law enforcement purposes.[115] Rising federal health care costs were a primary public concern at the time of the bill's enactment, and Congress found Medicare fraud to be a substantial part of the problem.[116] Consequently, in response to mounting public pressure to reduce these costs, Congress targeted Medicare fraud.[117] Congress granted the Attorney General administrative subpoena power for use in FBI fraud investigations that could obtain "any records or other things relevant to the [health care fraud] investigation."[118] These administrative subpoenas are identical to those of civil regulatory agencies, including their permissible scope, their enforcement through federal courts, the reasonableness standard federal courts must use in reviewing them, and the treatment of a motion to quash as an

---

the Intelligence Community Under the USA PATRIOT Act, 39 Am. Crim. L. Rev. 1261 (2002).

112. Hughes, *supra* note 28, at 594.

113. HIPAA § 248 is codified as 18 U.S.C. § 3486 (2000).

114. HIPAA, Pub. L. No. 104-191, § 248, 110 Stat. 1936 (1996) (codified at 18 U.S.C. § 3486).

115. Unlike civil regulatory agencies with enforcement power—such as the Internal Revenue Service ("IRS") or the Securities and Exchange Commission ("SEC")—the FBI is purely a law enforcement and domestic intelligence gathering institution. The FBI has no regulatory function at all; instead, the FBI builds criminal cases for federal prosecutors. The FBI agents and federal prosecutors working on a particular matter freely share all information relevant to the case. *See* Todd Masse & William Krouse, Congressional Research Serv., The FBI: Past, Present, and Future 14-17, 37 (Oct. 2, 2003), *available at* http://www.fas.org/irp/crs/RL32095.pdf.

116. DOJ Report, *supra* note 6, at 31.

117. *See id.*

118. 18 U.S.C. § 3486(a)(1)(B)(i).

appealable final order.[119] The two federal circuits that have faced challenges to administrative subpoenas under the statute upheld the subpoenas as reasonable under the Fourth Amendment without questioning the statute's validity.[120] As a result, this statute, with the blessing of the federal courts, enables the FBI to investigate health care fraud subject to the less strict Fourth Amendment standards for civil—not criminal—investigations.

2. The Federal Circuit Court Rulings on Section 248 of HIPAA

In *United States v. Bailey*,[121] the Fourth Circuit became the first federal appellate court to address the validity of an administrative subpoena issued under Section 248 of HIPAA. In *Bailey*, a doctor challenged four administrative subpoenas he received from the United States Attorney for the Western District of Virginia to investigate alleged insurance fraud.[122] The doctor argued that since he was the target of a criminal investigation, the Fourth Amendment required that the government demonstrate probable cause against him before demanding his records.[123] It would be unconstitutional, the doctor asserted, if the government could evade the Fourth Amendment probable cause requirement simply by issuing a subpoena instead of seeking a search warrant.[124] However, without

---

119. *See* DOJ Report, *supra* note 6, at 31-32. In this report, the Department of Justice recognized that these subpoenas permit investigators to obtain information that could have been obtained by grand jury subpoena, but the administrative subpoena avoids any delay and bypasses secrecy rules, making it a useful and flexible tool for these investigations. *Id.* at 35. In 2001, United States Attorneys' offices issued 2102 subpoenas under this statute. *Id.* at 34.

120. *See* Doe v. United States, 253 F.3d 256 (6th Cir. 2001); United States v. Bailey, 228 F.3d 341 (4th Cir. 2000).

121. 228 F.3d at 341.

122. *Id.* at 343-44. Each of the four subpoenas required the doctor to produce the following documents from the period between January 1992 and April 29, 1999:

> 1. All patient records and documentation concerning patients whose services were billed to [various insurance carriers], including complete medical files, patient appointment books, patient billing records, office sign-in sheets, and telephone messages in any form.
> 2. All purchase records and invoices reflecting . . . controlled substance purchases, DEA Official Order Forms, records of inventories, dispensing records . . . .
> 3. All original accounting and bank records, general ledgers, patient information/insurance cards, cash receipt and disbursement records, business ownership records and other items identifying sources of income from billings. . . .
> 4. All documents regarding health care plans' requirements for claim filing and record retention . . . .
> 5. All records of any controlled substance samples provided . . . .

Id. at 344.

123. Opening Brief of Appellant at 11-12, *Bailey*, 228 F.3d at 341 (No. 99-4870).

124. *Bailey*, 228 F.3d at 346. The doctor also challenged the subpoenas as unreasonable, overly broad, and in violation of his patients' doctor-patient privilege. *See id.* at 345.

addressing whether Congress could constitutionally permit the use of a lesser Fourth Amendment standard—reasonableness instead of probable cause—in criminal investigations, the court enforced the subpoenas.[125] As a consequence, the court set an important precedent allowing the government to use private information obtained without probable cause as the basis for a criminal prosecution.[126]

The U.S. Court of Appeals for the Sixth Circuit soon followed the *Bailey* court's lead. In *Doe v. United States*, the court also upheld administrative subpoenas issued to a podiatrist under Section 248 of HIPAA to investigate criminal fraud allegations.[127] The *Doe* court also rejected the petitioner's arguments that subpoenas under Section 248 of HIPAA violated the Fourth Amendment by giving agents and prosecutors access to private information without probable cause.[128] To support its conclusions, the *Doe* court reasoned that on-premises searches and inspections, including those conducted by administrative agencies, require probable cause, but because "[t]he immediacy and intrusiveness associated with a search are not present in [a] document request . . . the heightened requirement of probable cause is inapplicable" to any administrative subpoena.[129] The court did not differentiate between administrative subpoenas issued for civil rather than criminal purposes, merely noting that Congress granted the Department of Justice administrative subpoena power for use in health care fraud investigations without questioning the statute's validity.[130] As a result, the *Doe* court reinforced the Fourth Circuit's holding that administrative subpoenas could be used for purely criminal law enforcement purposes without any Fourth Amendment violation.[131]

125. *See id.* at 346-49. The court refused to distinguish the functions of civil administrative subpoenas and grand jury subpoenas. *Id.* at 346-47 (citing *United States v. Morton Salt Co.*, 338 U.S. 632 (1950), a case addressing the validity of purely civil administrative subpoenas, to support upholding the use of administrative subpoenas in a criminal investigation).

126. *See id.* at 347-48 ("While the Fourth Amendment protects people 'against unreasonable searches and seizures,' it imposes a probable cause requirement only on the issuance of warrants . . . . Thus, unless subpoenas are warrants, they are limited by the general reasonableness standard of the Fourth Amendment . . . , not by the probable cause requirement.").

127. Doe v. United States, 253 F.3d 256 (6th Cir. 2001).

128. *See id.* at 265.

129. *Id.* at 264.

130. *Id.* at 265.

131. *Id.* ("Both the Supreme Court and this circuit have long applied [the reasonableness] test when reviewing administrative subpoena requests, and we see no convincing basis upon which to distinguish these binding precedents simply because this subpoena was issued pursuant to a criminal, as opposed to civil, investigation.").

3. Congressional Limitations on Administrative Subpoena Power Under HIPAA

Although the statute and the case law may have undermined the Fourth Amendment rights of health care professionals under investigation for fraud, Congress did place an important limitation on administrative subpoena power in Section 248 of HIPAA to protect patients' privacy rights. The statute provides that a health care provider's subpoenaed records can only be used to investigate a violation of health care fraud laws.[132] Since health care is a highly regulated area in which detailed record keeping is often required by statute, administrative subpoena power over these records gives the FBI access to patients' private medical information as well as doctors' business and financial records.[133] However, the statute explicitly prohibits the FBI from using any patient's information in any other investigation unrelated to health care fraud.[134] While the statute gives the FBI access to many individuals' sensitive health care records, the FBI is strictly limited in its future use of this information for other investigations.

4. Informal Limitations on HIPAA Administrative Subpoena Power

The extent to which the Attorney General has delegated this subpoena power also presents a less formal check on the FBI's investigations. As permitted by the statute, the Attorney General delegated administrative subpoena power to all United States Attorneys and the Assistant Attorney General of the Criminal Division, who in turn delegated this authority to all Assistant United States Attorneys.[135] The Attorney General, however, has not delegated this power to the Director of the FBI, which the statute would also allow.[136] Because of this, FBI agents investigating Medicare fraud must rely on a federal prosecutor to issue a subpoena for the investigation.[137] While agents and prosecutors work closely together, a prosecutor usually holds gatekeeping power over coercive processes, like grand jury subpoenas, that an agent may need to build

---

132. 18 U.S.C. § 3486(e)(1) (2000).

133. *See* DOJ Report, *supra* note 6, at 35 (noting that the FBI has used these subpoenas to obtain records and documents from "hospitals, nursing homes and individual practitioners, including medical records, billing records, and cost reports").

134. 18 U.S.C. § 3486(e)(1)-(2). The United States Attorney's Manual specifically instructs prosecutors, who issue the HIPAA subpoenas, about the limitations on the future use of information obtained with the subpoenas. *See* Dept. of Justice, United States Attorney's Manual, 28 C.F.R. § 9-44.202[5] (2005).

135. *See* DOJ Report, *supra* note 6, at 34. In contrast, Congress has authorized the Secretary of the Treasury limited and non-delegable power to issue administrative subpoenas in cases where the Director of the Secret Service determines that there is an imminent threat against a Secret Service protectee. *Id.* at 38.

136. *Id.* at 34.

137. *Id.*

a case.[138] Since the Attorney General has not delegated administrative subpoena power to the FBI directly, United States Attorneys also end up in this gatekeeping position in Medicare fraud investigations conducted under Section 248 of HIPAA.[139] How frequently a prosecutor in the health care fraud context denies an agent's request for a subpoena undoubtedly varies,[140] but total deference to agents' requests is unlikely because prosecutors' and FBI agents' interests are not entirely aligned.[141] Because prosecutors seek to "build[] a professional reputation for legal acuity," they are risk averse and may not be willing to authorize an investigation that could be unsuccessful.[142] Judicial review of subpoenas heightens this risk aversion, because prosecutors encounter "'asymmetric accountability'"—that is, they are "more likely to face review and condemnation for authorizing action than for vetoing it."[143] Since prosecutors' and agents' interests in utilizing coercive processes can be incongruous, FBI agents' reliance on prosecutors to issue administrative subpoenas puts at least a small check on how and when agents actually use the subpoenas in investigations.

D. *Administrative Subpoena Power and Terrorism Investigations*

The Attorney General has successfully used administrative subpoena power to target Medicare fraud.[144] The subpoenas' effectiveness in the health care fraud context raises the question of whether Congress should grant the Attorney General—or the FBI—

---

138. Daniel Richman, *Prosecutors and Their Agents, Agents and Their Prosecutors*, 103 Colum. L. Rev. 749, 779-80 (2003) [hereinafter Richman, *Prosecutors and Their Agents*] (discussing prosecutorial controls of investigatory tools).

139. DOJ Report, *supra* note 6, at 34 (agents must rely on prosecutors to obtain Medicare fraud subpoenas). When Congress passed § 3486, the Attorney General recognized that Congress did not intend to give the FBI unlimited administrative subpoena power, and in anticipation of strict congressional oversight, the Attorney General self-imposed strict recordkeeping to track the use of the administrative subpoenas under § 3486. *See* Dept. of Justice, United States Attorney's Manual, 28 C.F.R. §§ 9-44.200 to 9-44.204.

140. Richman, *Prosecutors and Their Agents*, *supra* note 138, at 793 (discussing variations in prosecutor-agent relationships).

141. *See id.* at 778-87 (discussing prosecutorial controls of investigatory tools).

142. *Id.* at 784 (discussing prosecutorial controls of investigatory tools).

143. *Id.* at 785-86.

144. DOJ Report, *supra* note 6, at 35. The DOJ report found that

> [if] the statutory authority provided in 18 U.S.C. § 3486 [were] revoked, the use of a grand jury subpoena to obtain the same documents would decrease the opportunity to share information because of the protective provisions of Fed. R. Crim. P. 6(e). Loss of this information sharing capacity would hamper the efforts of the Attorney General to fulfill Congress' intent in providing the authority in HIPAA—to facilitate enforcement of federal statutes related to health care fraud and abuse and thereby improve the "availability and affordability of health insurance in the United States."

Id. In 2001, United States Attorneys issued 2102 administrative subpoenas for health care fraud investigations. *Id.* at 40.

additional administrative subpoena power for other types of criminal investigations.[145] The on-going national debate as to how the federal government can best fight terrorism now frames the question of whether the FBI should be given administrative subpoena power. After the September 11, 2001 terrorist attacks, Congress became extremely concerned with the FBI's ability to effectively combat terrorism, especially in terms of gathering and coordinating domestic intelligence to prevent another attack.[146] Without fundamental reforms to the FBI's structure and operations, the FBI could not effectively prevent future terrorist attacks.[147]

The USA PATRIOT Act,[148] passed only six weeks after the September 11, 2001 attacks, gave the Attorney General enhanced and widely delegable investigatory powers.[149] Section 215 of the PATRIOT Act, for example, enables government agents investigating international terrorism to bypass the Fourth Amendment's search warrant requirement.[150] However, the PATRIOT Act did not provide the FBI with similarly broad powers for domestic terrorism

---

145. *See* Updating the Law, *supra* note 7.

146. *See generally* 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks on the United States (2004) [hereinafter 9/11 Commission Report], *available at* http://www.gpoaccess.gov/911/; U.S. Senate Select Comm. on Intelligence and U.S. House Permanent Select Comm. on Intelligence, Joint Inquiry into Intelligence Community Activities Before and After the Terrorist Attacks of September 11, 2001 (December 2002) [hereinafter Joint Inquiry] (discussing factual findings and systemic weaknesses in the intelligence community leading up to the September 11, 2001 terrorist attacks), *available at* http://www.gpoaccess.gov/serialset/creports/911.html.

147. FBI Intelligence Reform, *supra* note 8, at 1-2. Two problems with the FBI's tradition and structure became immediately apparent. First, the FBI has "long favored its criminal justice mission over its national security mission." 9/11 Commission Report, *supra* note 146, at 423. As a consequence, FBI counter-terrorism programs lacked critical resources. *See* Joint Inquiry, *supra* note 146, at 336-45. Second, in response to domestic intelligence scandals in the 1960s, communication "walls" within the FBI separated criminal and intelligence investigations. FBI Intelligence Reform, *supra* note 8, at 14-15, 48. The FBI continues to work to refocus its resources and operations to be better equipped to prevent future terrorist attacks. *Id.* at 4-15.

148. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001) (to be codified at scattered sections of the U.S.C.).

149. Richard C. Leone, *The Quiet Republic: The Missing Debate About Civil Liberties After 9/11*, *in* The War on Our Freedoms: Civil Liberties in an Age of Terrorism 2, 7 (Richard C. Leone & Greg Anrig, Jr. eds., 2003).

150. *See* David Cole & James X. Dempsey, Terrorism and the Constitution: Sacrificing Civil Liberties in the Name of National Security 166 (2002) [hereinafter Terrorism and the Constitution]. Without making any showing of probable cause, if a government agent self-certifies that sensitive information in the form of "'any tangible things'" is sought for an international terrorism investigation, a judge from the Foreign Intelligence Surveillance Court can issue an order granting the agents access to the sought information. *Id.; see* § 215, 115 Stat. at 287-88.

investigations.[151] In an effort to equip the FBI with the necessary tools for effective counter-terrorism operations, bills proposed in the House and Senate would give the Attorney General unlimited administrative subpoena power for all terrorism investigations.[152] Part II explains these proposals to grant the FBI administrative subpoena power for terrorism investigations, as well as the Fourth Amendment implications of these proposals.

II. SHOULD THE FBI BE GRANTED ADMINISTRATIVE SUBPOENA POWER FOR TERRORISM INVESTIGATIONS?

President Bush, the Justice Department, and individual Congressmen and Senators have all pushed Congress to grant administrative subpoena power to the FBI for terrorism investigations. Proponents argue that the FBI should have the power to obtain on demand any documents or "tangible things" related to a domestic terrorism investigation.[153] Two bills to authorize administrative subpoena power for terrorism investigations have already been proposed in both houses of Congress.[154] The proposals would allow the FBI to issue its own subpoenas.[155] Subpoenaed parties that comply with the demand would be granted immunity from any resulting civil liability.[156] In circumstances where the Attorney General self-certifies that disclosure would endanger national security, subpoena recipients would be barred from disclosing to anyone, except legal counsel, that the subpoena was issued.[157] These bills immediately sparked heated debates in the House and Senate Judiciary Committee hearings.

The debate over whether administrative subpoena power should be given to the FBI for terrorism investigations raises three important questions. First, and most importantly, can this power be granted without undermining Fourth Amendment safeguards against unreasonable searches and seizures? Second, if Congress does give the FBI administrative subpoena power, what limitations, if any, should be imposed upon the FBI in using the power? Finally, on a practical level, would administrative subpoenas provide investigators

151. *See* Updating the Law, *supra* note 7.
152. *See* S. 2555, 108th Cong. (2004); H.R. 3037, 108th Cong. (2003).
153. *See* H.R. 3037.
154. S. 2555; H.R. 3037.
155. S. 2555; H.R. 3037. Although these bills name the Attorney General as the issuing authority, nothing in the bills would prevent the Attorney General from delegating this power to the FBI.
156. S. 2555; H.R. 3037. Senator Kyl, who proposed the Senate's version of the bill, explained that the bill would shield third-party subpoena recipients such as businesses from liability for breaching privacy agreements with customers in order to comply with the FBI's demand. 150 Cong. Rec. S7178 (daily ed. June 22, 2004) (statement of Sen. Kyl to introduce S. 2555).
157. 150 Cong. Rec. S7178 (daily ed. June 22, 2004) (statement of Sen. Kyl to introduce S. 2555).

with too much information to be useful as an effective investigatory tool? Parts II.A, II.B, and II.C examine these questions in turn.

A. *Administrative Subpoena Power, Terrorism Investigations, and Fourth Amendment Privacy Rights*

Although giving the FBI administrative subpoena power for terrorism investigations would be an unprecedented grant of power, supporters argue that Fourth Amendment rights would not be infringed.[158] According to the federal appellate courts that have examined the use of administrative subpoenas in criminal health care fraud investigations, the subpoenas do not violate the Fourth Amendment.[159] Administrative subpoena power could not be abused by investigators because the subpoenas would be subject to judicial review and could only be enforced by a federal court.[160] As with all administrative subpoenas, any subpoenaed party could bring a challenge to the demand in federal court,[161] subject to the *Powell* reasonableness test,[162] and a denial of a motion to quash would be immediately appealable as a final order.[163] Since judicial review would ensure that only the reasonable subpoenas are enforced, use of the subpoenas would not violate Fourth Amendment rights.[164] Critics respond to these proposals with two concerns.

1. Concerns About Probable Cause Versus Reasonableness

First, as in the health care context, administrative subpoenas for terrorism investigations would permit the government to use private information obtained without probable cause in a criminal investigation.[165] However, differences between health care fraud and terrorism indicate that while a relaxed Fourth Amendment standard

158. *See Tools to Fight Terrorism: Subpoena Authority and Pretrial Detention of Terrorists: Hearing Before the United States Senate Judiciary Comm., Subcomm. on Terrorism, Tech. and Homeland Sec.*, 108th Cong. (2004) [hereinafter Brand Testimony] (testimony of Rachel Brand, Principal Deputy Assistant Attorney General, Office of Legal Policy, United States Department of Justice), *available at* http://judiciary.senate.gov/hearing.cfm?id=1235; 150 Cong. Rec. S7178-79 (daily ed. June 22, 2004) (statement of Sen. Kyl regarding S. 2555).

159. *See* Doe v. United States, 253 F.3d 256 (6th Cir. 2001) (upholding administrative subpoena power for health care fraud investigation); United States v. Bailey, 228 F.3d 341 (4th Cir. 2000) (same).

160. Brand Testimony, *supra* note 158.

161. 150 Cong. Rec. S7179 (daily ed. June 22, 2004) (statement of Sen. Kyl explaining the provisions of S. 2555).

162. *See supra* note 86 and accompanying text.

163. *See supra* note 101 and accompanying text.

164. 150 Cong. Rec. S7179 (daily ed. June 22, 2004).

165. For examples of the use of administrative subpoenas in the context of health care fraud, see *Doe v. United States*, 253 F.3d 256 (6th Cir. 2001), and *United States v. Bailey*, 228 F.3d 341 (6th Cir. 2000). See *supra* Part I.C.2 for a discussion of these holdings.

may be appropriate for health care investigations, this may not be the case for terrorism investigations. A health care fraud investigation is similar to a regulatory agency investigation because, since the evidence of wrongdoing only exists in a provider's business and financial records, a probable cause requirement would impede an effective investigation.[166] A terrorism investigation, however, could be pursued by using many tactics; useful information could likely come from many sources, not just one determinate set of business records.[167] As a result, applying a relaxed Fourth Amendment standard to terrorism investigations may not always be necessary. However, applying this relaxed standard to all terrorism investigations would enable the FBI to evade Fourth Amendment probable cause requirements to access suspects' private information in a wide range of circumstances.

Adding to the gravity of this Fourth Amendment problem, critics note that terrorism administrative subpoenas would give the FBI access to an unprecedented amount of private information without probable cause.[168] Administrative subpoenas provide investigators

166. *See* Gellhorn & Levin, *supra* note 84, at 130; *see also supra* text accompanying note 84.

167. *See generally* Joint Inquiry, *supra* note 146 (detailing the many different types of operations and strategies necessary to gather information to fully investigate suspected terrorists).

168. The closest Congress has come to granting the FBI such broad power is in section 218 of the PATRIOT Act, which permits the Foreign Intelligence Surveillance Act ("FISA") courts to issue warrants for surveillance without probable cause if foreign intelligence gathering is "a significant purpose" of the surveillance. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272, 291 (2001) (to be codified at scattered sections of the U.S.C.); *see* Charles Doyle, Congressional Research Serv., The USA PATRIOT Act: A Legal Analysis 9 (Apr. 15, 2002), *available at* http://fpc.state.gov/documents/organization/10092.pdf. Congress established the FISA courts in 1978, but before the PATRIOT Act, FISA warrants required certification that "the purpose of the surveillance is to obtain foreign intelligence information." 50 U.S.C. § 1804(a)(7)(B) (2000) (amended 2001); *see* Doyle, *supra*, at 8. The PATRIOT Act amendment enables government agents to use the information obtained with a FISA warrant for domestic criminal law enforcement purposes by eliminating the barriers between criminal investigations and foreign intelligence operations that developed out of court rulings and the Justice Department's interpretation of FISA requirements. *See* 9/11 Commission Report, *supra* note 146, at 78-80. Although "[f]acilitating closer cooperation between criminal investigators and foreign intelligence collectors is probably not a controversial intention in itself," critics take issue with section 218 because it allows government agents to obtain warrants to conduct surveillance that could ultimately be used in a criminal prosecution without a showing of probable cause. Reg Whitaker, *After 9/11: A Surveillance State?*, *in* Lost Liberties: Ashcroft and the Assault on Personal Freedom 52, 59-61 (Cynthia Brown ed., 2003). Critics view this as an end-run around the Fourth Amendment requirements for gathering information that will be used in a criminal prosecution. *See* Nancy Chang, Silencing Political Dissent 55-59 (2002). However, at the present, this power is still tied to foreign intelligence information and no similar power exists for gathering domestic intelligence; additionally, because of

with access to all information "relevant to" the investigation.[169] But because of the differences between Medicare fraud and terrorism, administrative subpoenas in the terrorism context would give the FBI access to significantly more information.[170] Since Congress defined health care fraud narrowly, the range of documents "relevant to" the crime is limited to the provider's professional, business, and financial records.[171] However, as the September 11, 2001 attacks unfortunately demonstrated, and as the federal international terrorism statute reflects,[172] the range of information that could be "related to" terrorist activities is infinitely broad—anything from flight school enrollment to rental car reservations. Administrative subpoena power could be an effective investigatory tool for the FBI because it would provide broad access to private information, but the information would come at the cost of individuals' Fourth Amendment privacy rights in many different contexts.[173]

---

the controversial nature of section 218, it is one of the PATRIOT Act provisions that will "sunset" on December 31, 2005 without further action from Congress. *See* Doyle, *supra*, at 10, 13-14.

169. 18 U.S.C. § 3486(a)(1)(B)(i) (2000); *see also Doe*, 253 F.3d at 266 (upholding as reasonable a health care fraud administrative subpoena because the proper scope of an administrative subpoena is "'evidence . . . [that is] not plainly incompetent or irrelevant to any lawful purpose of the [agency] in the discharge of [its] duties'" (quoting Endicott Johnson Corp. v. Perkins, 317 U.S. 501, 509 (1943)).

170. Under HIPAA, federal health care fraud is limited to knowingly and willfully (1) defrauding any health care benefit program by means of false representations; (2) making false statements regarding a health care benefit program; (3) embezzling, converting, or stealing any funds, property, or assets of a health care benefit program; or (4) obstructing, delaying, preventing, or misleading federal health care fraud investigators. *See* Jonathan Cone et al., *Health Care Fraud*, 40 Am. Crim. L. Rev. 713, 749-50 (2003). In comparison, the federal statute defining international terrorism, 18 U.S.C. § 2332b, is much broader and covers many different types of activities.

171. *See Doe*, 253 F.3d at 259-61; United States v. Bailey, 228 F.3d 341, 344 (4th Cir. 2000). The *Doe* court upheld the reasonableness of a Medicare administrative subpoena that requested the defendant-podiatrist's health care related bank and financial records, tax returns, documents and files regarding patient referrals, academic transcripts from all medical training, all documents concerning ethics, professional responsibility, and medical-billing issues within podiatrist's possession, and all professional publications received by the podiatrist. *Doe*, 253 F.3d at 259-61. The *Bailey* court upheld the reasonableness of a Medicare administrative subpoena that requested the defendant-doctor's patient records where the doctor's services were billed to specified health insurances companies, purchase records and invoices reflecting controlled substance purchases, accounting and bank records, documents regarding health care plans' requirements for claim filing, and records of samples of controlled substances received from drug companies. *Bailey*, 228 F.3d at 344.

172. 18 U.S.C. § 2332b.

173. As Senator Patrick Leahy pointed out in a Senate Judiciary Committee hearing regarding the use of administrative subpoenas in terrorism investigations, "[t]here are a handful of administrative subpoena powers that are in the criminal code. Because criminal proceedings are unique, and the ability to do harm to the target of a criminal investigation simply for being investigated is great, these existing powers are carefully crafted, limited and statute specific." *Tools to Fight Terrorism: Subpoena Authority and Pretrial Detention of Terrorists: Hearing Before the United*

2. Concerns About the Effectiveness of Judicial Review

Second, critics argue, in practice, judicial safeguards would not protect individuals' privacy from unreasonable terrorism administrative subpoenas.[174] Even if a reasonableness standard would not violate the Fourth Amendment, judicial review would not weed out unreasonable subpoenas because recipients have no incentive to challenge the demands.[175] To challenge a subpoena, the recipient faces a high burden of proof to prevail and must bear all litigation costs.[176] While this alone is not significant, as courts accept administrative subpoenas as legitimate in other contexts despite these conditions,[177] using these subpoenas in terrorism investigations would be subtly—but critically—different. When the FBI subpoenas a health care provider's records in a Medicare fraud investigation, that health care provider is under investigation.[178] However, if the FBI were to subpoena an internet service provider's business records for a terrorism investigation, the investigation would likely be focused on one of the company's clients, not the company itself.[179] The internet service provider would be a third party, not under investigation, and would be shielded from all civil liability,[180] including lawsuits for violating privacy agreements with customers.[181] Further, the customers themselves, even if alerted to the demand, do not have standing to challenge the demand.[182] While the subpoenaed health care provider would have an incentive—the provider's own future criminal liability—to bear the costs and the high risk of losing a motion to quash the subpoena, a third party insulated from liability has no similarly compelling reason to resist compliance with even unreasonable subpoenas.[183] In the context of terrorism investigations,

---

States Senate Judiciary Comm., 108th Cong. (2004) [hereinafter Leahy Testimony] (statement of Senator Patrick Leahy, ranking Democratic member of the United States Senate Judiciary Committee), *available at* http://judiciary.senate.gov/hearing.cfm?id=1235.

174. *See Tools to Fight Terrorism: Subpoena Authority and Pretrial Detention of Terrorists: Hearing Before the United States Senate Comm. on the Judiciary*, 108th Cong. (2004) [hereinafter Robinson Testimony] (testimony of James Robinson, Former Assistant Attorney General, United States Department of Justice, 1998-2001), *available at* http://judiciary.senate.gov/hearing.cfm?id=1235.

175. *Id.*

176. *Id.; see supra* notes 64-69 and accompanying text.

177. *See supra* notes 90-96 and accompanying text.

178. Ctr. for Democracy & Technology, Administrative Subpoenas for the FBI: A Grab for Unchecked Executive Power (Sept. 24, 2003), *at* http://www.cdt.org/security/usapatriot/030924cdt.shtml [hereinafter Unchecked Power].

179. *See id.*

180. *See supra* note 156 and accompanying text.

181. *See* Unchecked Power, *supra* note 178.

182. *See supra* note 37 and accompanying text.

183. *See* Unchecked Power, *supra* note 178. As Professor Orin Kerr points out, the cost to a third party, such as an internet service provider, of providing information to

because third party subpoena recipients have no incentive to challenge the FBI's demands, judicial review cannot actually protect the privacy rights of individuals under investigation.[184]

Also, even if subpoenaed parties did have an incentive to resist compliance, they may not know that they could challenge the demand. In the context of Medicare fraud, since health care providers are sophisticated parties and the field is highly regulated, providers likely know their rights under HIPAA.[185] In contrast, since the range of businesses that may possess information about an individual targeted by an FBI terrorism investigation is limitless, there is no similar guarantee in this context that a subpoena recipient will be a sophisticated party.[186] When faced with a demand from the FBI, especially if the subpoena mandates complete secrecy, a party may not know that the demand could be challenged in court. Again, in the terrorism context, the availability of judicial review may not work to weed out unreasonable subpoenas and protect individuals' privacy rights.

Relatedly, subpoena recipients unsure of their rights could be too intimidated to resist the FBI's demand. In a different context, the Supreme Court held that if an agency's official demand for cooperation with government authorities implies that noncompliance is not an option, the technical legality of noncompliance is, on its own, an inadequate safeguard of individuals' rights to challenge the demand.[187] In *Bantam Books, Inc. v. Sullivan*, the Court examined a Rhode Island state legislative provision that established a commission

---

respond to a government subpoena often decreases as the amount of information demanded increases. Orin S. Kerr, *Digital Evidence and the New Criminal Procedure*, 105 Colum. L. Rev 279, 293-94 (2005). This speaks to both the incentive of a third-party subpoena recipient to challenge a demand as unreasonable and the toothlessness of the *Powell* "burdensomeness" factor in assessing a subpoena's reasonableness. *See id.* Professor Kerr further argues that traditional criminal procedures do not translate to adequately protect privacy rights in criminal investigations and prosecutions that use digital evidence, and he proposes a higher legal threshold to compel disclosure of such evidence. *Id.* at 294, 309.

184. *See* Unchecked Power, *supra* note 178.

185. *Id.*

186. *Cf.* Terrorism and the Constitution, *supra* note 150, at 159 (arguing that post-September 11, 2001 changes to laws governing surveillance and information-gathering will likely target Arab and Muslim immigrants); David Cole, *The Course of Least Resistance: Repeating History in the War on Terrorism*, *in* Lost Liberties: Ashcroft and the Assault on Personal Freedom, *supra* note 168, at 13, 30-31 (arguing that, as in past times of threat, including both World Wars, the Cold War, and Vietnam, post-September 11, 2001 security measures enable the government to target a vulnerable minority, namely Arab and Muslim foreign nationals); Christopher Edley Jr., *The New American Dilemma: Racial Profiling Post-9/11*, *in* The War on Our Freedoms: Civil Liberties in an Age of Terrorism, *supra* note 149, at 170, 185 (arguing that post-September 11, 2001 government surveillance will likely disproportionately target Muslims, Arabs, and South Asians, sweeping many private individuals into the government's net of suspicion).

187. Bantam Books, Inc. v. Sullivan, 372 U.S. 58, 68-69 (1963).

to prevent the sale of obscene publications to minors.[188] As part of its duties, the commission would, on official stationery, notify book distributors that the commission had deemed some of the distributor's materials obscene, thank the recipient in advance for cooperating with authorities to prevent sale of the materials to minors, remind the recipient that the commission's duty was to recommend prosecution upon discovering such sales, and mention that the commission's lists of objectionable materials would be circulated to local police departments.[189] The Court held that although a distributor's "refusal to 'cooperate' [with a letter from the commission] would have violated no law . . . ., [p]eople do not lightly disregard public officers' thinly veiled threats to institute criminal proceedings against them if they do not come around [and comply with the demand]."[190] An FBI administrative subpoena in a terrorism investigation could have a similar effect on recipients. A subpoenaed party may comply out of fear of repercussions for noncompliance, whether or not the recipient knew that the demand could be challenged. If intimidated subpoena recipients will not challenge potentially unreasonable subpoenas, the judicial review safeguard would be further undermined.

B. *What Limitations, if Any, Should Be Placed on the FBI's Use of Information Obtained by Administrative Subpoenas?*

If Congress grants administrative subpoena power to the FBI for terrorism investigations, the question then becomes how, if at all, Congress should limit the power. Advocates in favor of granting the FBI terrorism subpoena power regularly cite the effectiveness of administrative subpoenas in investigating and prosecuting Medicare fraud to justify using the power in a wide range of terrorism investigations.[191] Critics, however, point out that Congress subjected Medicare fraud subpoena power to strict limitations to protect the privacy of patients uninvolved in the fraud.[192] In the terrorism context, without clearly defined boundaries, critics argue, administrative subpoena power would give the FBI extraordinary power that could be too easily abused or overused.[193] In its report, the 9/11 Commission stated that in considering the future tools necessary to fight terrorism, in light of concerns for civil liberties, "[i]f [an executive branch] power is granted, there must be adequate

188. *Id.* at 59.
189. *Id.* at 62-63.
190. *Id.* at 68.
191. *See* Updating the Law, *supra* note 7.
192. *See* Unchecked Power, *supra* note 178.
193. *See A Review of Counter-Terrorism Legislation and Proposals, Including the USA PATRIOT Act and the SAFE Act: Hearing Before the United States Senate Judiciary Comm.*, 108th Cong. (2004) (testimony of Bob Barr, Former Member of Congress, 1995-2003, for the Seventh District of Georgia), *available at* http://judiciary.senate.gov/hearing.cfm?id=1312.

guidelines and oversight to properly confine its use."[194] Using the 9/11 Commission's recommendation as a starting point, and drawing upon the FBI's experience with Medicare fraud administrative subpoenas, two questions arise regarding the necessary limits on FBI subpoena power.

1. Governmental Use of Information Accessed Through Administrative Subpoenas

The usefulness of the information obtained by an administrative subpoena would be different in a health care investigation and in a terrorism investigation. An administrative subpoena is useful to Medicare fraud investigators because it provides access to a determinative set of documents: the health care provider's business and financial records.[195] After an investigation ends, however, the statute requires that the seized records cannot be used further unless they reveal evidence of additional Medicare fraud.[196] In the health care context, Congress outlawed using any confidential information accessed by administrative subpoenas in a larger criminal investigation because such an investigation would compromise the privacy rights of patients not implicated in the fraud.[197]

In the terrorism context, however, the vast amounts of information obtained by administrative subpoenas would likely be used for data mining.[198] Objectively, data mining presents terrorism investigators with a useful tool because it picks out significant patterns in huge quantities of information.[199] Data mining enables investigators to "connect the dots" between seemingly insignificant events.[200] In the months leading up to September 11, 2001, the FBI failed to notice and connect significant pieces of information that could have uncovered the terrorist plot,[201] in part because of insufficient information analysis.[202] As Mary DeRosa points out in her report on data mining for the Center for Strategic and International Studies, basic data

194. 9/11 Commission Report, *supra* note 146, at 394-95.

195. *See supra* notes 166, 171 and accompanying text.

196. 18 U.S.C. § 3486(e)(1) (2000); *see* A. Craig Eddy, *The Effect of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) on Health Care Fraud in Montana*, 61 Mont. L. Rev. 175, 202 (2000) (explaining the investigatory subpoena power granted to federal health care fraud investigators under HIPAA).

197. *See* DOJ Report, *supra* note 6, at 33.

198. *See* Mary DeRosa, Ctr. for Strategic and Int'l Studies, Data Mining and Data Analysis for Counterterrorism 14 (2004) (noting that although data mining on its own does not give the government greater access to private information, data mining techniques employed for counterterrorism purposes would be applied to data within the government's possession), *available at* http://www.csis.org/tech/2004_counterterrorism.pdf.

199. *Id.* at 3.

200. *Id.* at 13.

201. Joint Inquiry, *supra* note 146, at 10-33.

202. *Id.* at 59, 336-39.

mining using government watch list information, airline reservation records, and aggregated publicly available data would have linked together and identified all nineteen of the September 11, 2001 hijackers.[203] Because of the growing importance of subtle and superficially unconnected pieces of information, computer-based data mining could provide valuable assistance to investigators faced with large quantities of potentially relevant information.

Additionally, as Professor Philip Heymann points out, as the FBI shifts its focus from ex-post criminal investigations to ex-ante terrorism investigations, the FBI must also recognize that terrorism prevention requires a much more complete set of information than is necessary to solve a crime after the fact.[204] Investigation of a crime after it occurs can take years, and the crime scene itself can often provide valuable leads.[205] Counter-terrorism investigators working to prevent an attack, however, must tackle the much more difficult task of finding "traces of a plan, [as opposed to] traces of a completed event" under the pressure of a serious deadline.[206] Additionally, although convicting most of the perpetrators of a successful crime could be considered a success, "locking up less than a critical mass of a group planning a future crime has to be considered a failure."[207] Since terrorism investigators must find patterns in huge quantities of data,[208] data mining of information obtained through administrative subpoenas could significantly boost the success of these investigations.[209]

---

203. DeRosa, *supra* note 198, at 6-8 (explaining that all nineteen of the September 11, 2001 hijackers were within three degrees of separation from one another, and that they could have been connected simply by using then-current U.S. government terrorist watch list information, flight reservation contact information, frequent flyer numbers, and public records of the hijackers' past addresses). However, although the FBI made some glaring mistakes, the September 11, 2001 hijackers also intentionally avoided activities, such as affiliating with radical political groups, that traditionally would have flagged them for special attention by authorities. *See* 9/11 Commission Report, *supra* note 146, at 254-77 (describing "the summer of threat" leading up to the attacks during which "the system was blinking red," but viable leads and terrorists' mistakes were not capitalized upon by any federal agency responsible for counter-terrorism); Terrorism and the Constitution, *supra* note 150, at 167 (noting that the September 11, 2001 hijackers avoided drawing attention to themselves by intentionally avoiding radical political affiliations).

204. Philip B. Heymann, Terrorism, Freedom, and Security 64-65 (2003).

205. *Id.*

206. *Id.* at 65.

207. *Id.*

208. *See id.*

209. Despite its usefulness to detect suspicious patterns in huge quantities of data, data mining still has important limitations. Although data mining can identify patterns and relationships in large data sets, analysts are still necessary to assess the patterns' significance. *See* Jeffrey W. Seifert, Congressional Research Serv., Data Mining: An Overview 3 (2004), *available at* http://www.fas.org/irp/crs/RL31798.pdf. Also, only patterns already believed to be suspicious will be identified by pattern-based data mining because formulating the queries inherently requires a judgment of what constitutes a suspicious behavior pattern. *See* Heymann, *supra* note 204, at 72.

Recognizing that data mining could provide terrorism investigators with useful information, critics nonetheless argue that the possibility of "mission creep" further augments the Fourth Amendment concerns surrounding administrative subpoenas.[210] An assembled network of information set up for data mining could easily be used to fight crime other than terrorism.[211] If data mining proves to be an effective tool to fight terrorism, Congress could be tempted to permit its use to help investigate the next type of high profile illegal behavior.[212] However, since administrative subpoenas access information without probable cause, mission creep could lead to criminal prosecutions for crimes other than terrorism on the basis of private information obtained without probable cause.[213] Data mining experts admit that without government-wide guidelines for the future use of information collected by administrative subpoena, mission creep could definitely occur.[214] Although such crimes may

---

210. In his report, Jeffrey Seifert pointed out that

> [m]ission creep is one of the leading risks of data mining cited by civil libertarians, and represents how control over one's information can be a tenuous proposition. Mission creep refers to the use of data for purposes other than that for which the data was originally collected. This can occur regardless of whether the data was provided voluntarily by the individual or was collected through other means.

Seifert, *supra* note 209, at 12. The possibility of mission creep also surrounds the debate over national ID cards. *See* Kathleen M. Sullivan, *Under a Watchful Eye: Incursions on Personal Privacy*, *in* The War on Our Freedoms: Civil Liberties in an Age of Terrorism, *supra* note 149, at 128, 145 ("A national database, however benignly motivated, will lie about waiting to be used or misused given the right conditions .... On the 'loaded weapon' view, liberty is best protected when data, like political sovereignty, is sufficiently decentralized.").

211. *See* Seifert, *supra* note 209, at 13 ("[S]ome experts suggest that anti-terrorism data mining applications might also be useful for combating other types of crime as well.").

212. DeRosa, *supra* note 198, at 16. "At any time, another type of illegal behavior could take on a high profile, and authorities will be under pressure to expand the use of these techniques, for example, to help investigate other violent criminals, immigration law violators, or even 'deadbeat dads.'" *Id; see also* Dep't of Defense, Report of the Technology and Privacy Advisory Committee, Safeguarding Privacy in the Fight Against Terrorism 7 (March 2004) ("We conclude that advanced information technology—including data mining—is a vital tool in the fight against terrorism, but in developing and using that tool the government must—and can—protect privacy and fundamental civil liberties."), *available at* http://www.cdt.org/security/usapatriot/20040300tapac.pdf.

213. This concern highlights a crucial difference between administrative subpoenas and grand jury subpoenas: Because of the strict grand jury secrecy rules, data mining of information obtained through grand jury subpoenas would be extremely unlikely. *See supra* notes 55-63 and accompanying text.

214. DeRosa, *supra* note 198, at 16.

> No matter how legitimate the reason for collection or how careful the initial use, information can take on a life of its own if not controlled, and it can be used by others for reasons unrelated to the initial collection. Currently, no government-wide guidelines exist for collection, use, retention, and dissemination of private data, and oversight of these activities is inconsistent at best.

legitimately demand authorities' attention, "there will be less opportunity for robust public debate on . . . expanded use" of "new tools once they have been implemented for one purpose"—that is, Congress may be unable to resist sliding down a slippery slope.[215] If Congress were to authorize the use of data mining from administrative subpoenas for other types of crime, the breach of all individuals' privacy would be vastly expanded, and targeted individuals would again be subject to prosecution based upon private information obtained without probable cause.

2. Delegation of Authority to Issue Administrative Subpoenas

Second, how far down the chain of command would subpoena issuing power be delegated? The bills proposed in Congress would give the Attorney General administrative subpoena power that could be delegated to the director of the FBI, who could further delegate the power to agents.[216] In the health care context, since the Attorney General has not delegated this power to the FBI, prosecutors' gatekeeping power to issue the subpoenas places an informal check on their indiscriminate use.[217] Since prosecutors face "asymmetric accountability," their interests are not wholly aligned with investigators' interests, and a prosecutor may be less likely to risk issuing a subpoena for an investigation unlikely to bear fruit.[218] Similarly, in the terrorism context, limiting administrative subpoena power to traditionally risk-averse prosecutors would provide an additional check on abuses of this power.[219] Although the strength of prosecutors' gatekeeping power would hinge on their response to the pressures of post-September 11, 2001 terrorism investigations, prosecutors could still provide a check on agents conducting overreaching terrorism investigations.

Id.

215. *Id.; see also* Stephen J. Schulhofer, *No Checks, No Balances: Discarding Bedrock Constitutional Principles*, *in* The War on Our Freedoms: Civil Liberties in an Age of Terrorism, *supra* note 149, at 74, 84-85 (noting that, technically, many of the enhanced powers Congress granted the FBI since September 11, 2001 could be used to investigate crimes other than terrorism). Although the restrictions that Congress placed upon Medicare administrative subpoenas did strictly limit the future use of information obtained by the subpoenas, administrative subpoenas in the terrorism context would provide the government with a much broader range of information that could prove valuable in many more types of criminal investigations. *See supra* notes 168-73 and accompanying text.

216. *See* S. 2555, 108th Cong. (2004); H.R. 3037, 108th Cong. (2003).

217. *See supra* notes 135-43 and accompanying text.

218. *See supra* notes 135-43 and accompanying text.

219. Arguably, however, prosecutors in post-September 11, 2001 terrorism investigations may try to overcompensate—that is, prosecutors' risk aversion would become inclined to take risks in these investigations. If so, prosecutors would not provide the same check on agents' eagerness to use administrative subpoenas as in the health care fraud context.

C. *Practical Concerns: Would Administrative Subpoenas Provide Too Much Information?*

Finally, on a practical level, critics also worry that broad investigatory tools like administrative subpoenas would provide terrorism investigators with too much irrelevant information for the subpoenas to be useful as an investigatory tool.[220] Before September 11, 2001, the FBI's terrorism intelligence capability suffered due to institutional shortcomings.[221] The FBI's decentralized system of collecting intelligence, the lack of communication both within the FBI field offices and with other agencies in possession of critical information, and an underfunded counter-terrorism program placed low on the agency's priority list all contributed to the FBI's failure to piece together clues about the impending attacks.[222] But while agency reorganization can shift the FBI's focus to counter-terrorism, unfocused and overbroad investigatory tools that sweep up large quantities of irrelevant information could waste analysts' time as well as other valuable resources.[223] Although administrative subpoenas could give terrorism investigators some important information, since the subpoenas will also cover inordinate amounts of unrelated information, their benefit as an investigatory tool could be outweighed by the inefficiencies they impose upon intelligence analysts.[224]

III. USING ADMINISTRATIVE SUBPOENAS FOR CRIMINAL INVESTIGATIONS WOULD SERIOUSLY UNDERMINE FOURTH AMENDMENT PRIVACY RIGHTS

In the context of a criminal investigation, administrative subpoenas conflict with the Fourth Amendment because the subpoenas allow

---

220. *See* Schulhofer, *supra* note 215, at 85. Professor Schulhofer noted that

> [i]t is now well known that before September 11 the FBI and the Central Intelligence Agency had important clues to the plot in hand, but as one FBI agent put it, "We didn't know what we knew." Since a large part of what we lack is not raw data but the ability to separate significant intelligence from so-called noise, pulling more information into government files will not help and may aggravate the difficulty.

Id. at 86.

221. *See* Joint Inquiry, *supra* note 146, at 79-81.

222. *See* 9/11 Commission Report, *supra* note 146, at 74-80; *see also* Joint Inquiry, *supra* note 146, at 77-90, 336-45, 358.

223. *See* Whitaker, *supra* note 168, at 68 (noting that "as a general rule, the collection capacity of intelligence agencies has outstripped their analytical capacities").

224. *See id.* (arguing that "[some investigatory] [s]chemes . . . actually threaten to worsen this [pre-9/11] imbalance [between available information and resources for analysis], [by] swamping overworked analysts with too much information, almost all of it irrelevant, but requiring processing"); *see also* Edley, *supra* note 186, at 185 ("[W]hile it is true that the potential horror [of terrorism] exceeds that of conventional crime, that makes it all the more important that the investigation and enforcement strategies be *effective*, not merely *political and symbolic*.").

government agents to bypass the probable cause requirement to obtain private information. Although holding investigators to a lower Fourth Amendment standard may be justified for some types of criminal investigations, such as health care fraud,[225] Congress must carefully assess whether terrorism investigations require similar intrusions on Fourth Amendment rights. The degree to which the subpoenas would be an effective and useful investigatory tool should be taken into account.[226] Congress must also recognize that the use of administrative subpoenas in terrorism investigations would seriously undermine individuals' Fourth Amendment rights in other criminal investigations, and Congress must be willing to justify these consequences to the federal courts and to the public. However, if Congress does grant the FBI administrative subpoena power for terrorism investigations, Congress should place limitations on the future use of information obtained with the subpoenas to avoid further and unnecessary undermining of the probable cause requirement for criminal investigations. Although federal courts may still strike down such a grant of power, restrictions that prevent the expansion of this power to non-terrorism contexts would better comport with Fourth Amendment policies.

A. *Health Care Fraud Is the Exception, Not the Rule: The Justification for Abrogating Fourth Amendment Rights in Health Care Fraud Investigations Is Not Compelling in Other Contexts*

Under the Supreme Court's long-standing interpretation of the Fourth Amendment, government agents acting with nothing more than mere suspicion cannot legitimately invade individuals' privacy.[227] The probable cause requirement reflects the framers' and ratifiers' belief that capricious state action is unacceptable, and probable cause sets a threshold below which state action is deemed arbitrary.[228] Although the strict probable cause requirement could prevent investigators from pursuing every available lead in an important criminal investigation, the requirement protects innocent people from unfair and arbitrary state privacy intrusions.[229] According to long-standing Fourth Amendment principles, using administrative subpoenas for criminal investigations would violate the privacy rights of huge numbers of people.[230] Anyone, guilty or innocent, whose private information would be accessed by the subpoenas has the right

225. *See* Doe v. United States, 253 F.3d 256, 263-65 (6th Cir. 2001); United States v. Bailey, 228 F.3d 341, 346-47 (4th Cir. 2000); *supra* Parts I.C.1-C.2.

226. *See supra* Part II.C.

227. *See supra* Part I.A.1.

228. *See supra* notes 13-19 and accompanying text.

229. *See supra* notes 13-19 and accompanying text.

230. *See* Amsterdam, *supra* note 15, at 411; *supra* notes 13-27 and accompanying text. For an overview of the historical context of the probable cause requirements, see Gould & Stern, *supra* note 14, at 792-93 & n.65.

to keep that information private unless the state can demonstrate probable cause for suspicion.[231]

By permitting the use of administrative subpoenas in health care fraud investigations under HIPAA, Congress and the federal appellate courts opened the door for criminal prosecutions based upon evidence found in private documents that were obtained without probable cause, seemingly in violation of the Fourth Amendment.[232] However, holding investigators to a lower Fourth Amendment reasonableness standard in a health care fraud investigation makes sense because a health care fraud investigation and an administrative regulatory investigation present similar difficulties for investigators.[233] In both administrative regulatory investigations and health care fraud investigations, requiring probable cause could entirely undermine investigators' efforts because private records are the determinative evidence in the investigation; without access to these records, investigators may never have probable cause.[234] But this justification is not persuasive in the context of other criminal investigations, including terrorism investigations, where investigators receive critical information from many different sources.[235] Without equally compelling justifications, administrative subpoenas cannot be used in terrorism and other similar investigations without seriously abrogating individuals' Fourth Amendment rights.

B. *From Probable Cause to Abandoning All Safeguards: The Secondary Problems of Judicial Review and Mission Creep*

In addition to conflicting with long-standing principles of Fourth Amendment rights, terrorism administrative subpoenas present serious secondary implications for Fourth Amendment rights. Two main concerns arise: judicial review and mission creep.

First, granting administrative subpoena power for terrorism investigations would do more than merely substitute a reasonableness standard of review under the Fourth Amendment for the probable cause standard. Due to the differences between health care fraud and terrorism investigations, administrative subpoenas in the terrorism context would afford suspects no Fourth Amendment protection at all because judicial review will not work to weed out unreasonable demands.[236] When investigators issue an administrative subpoena under HIPAA, the recipient is the doctor who is under

231. *See* Amsterdam, *supra* note 15, at 411; *supra* notes 13-27 and accompanying text.

232. *See supra* Part I.C.1.

233. *Compare supra* notes 82-84 and accompanying text, *with supra* notes 165-67 and accompanying text.

234. *See supra* note 166 and accompanying text.

235. *See supra* note 167 and accompanying text.

236. *See supra* Part II.A.2.

investigation.[237] If the demand is unreasonable—if it asks for information unrelated to health care fraud, for example—it is in the doctor-recipient's own interest to challenge the subpoena to protect the private records from unreasonable government intrusion.[238]

However, in the terrorism context, the subpoena recipients will likely be third parties not under investigation, such as internet service providers, credit card companies, or, as in the hypothetical above, retailers.[239] Under the proposed legislation, third parties would be absolved from any liability arising from divulging information requested by the subpoena.[240] While these third parties might challenge a demand that requires access to voluminous amounts of information that would be expensive to produce, they have no incentive to incur the costs of litigating a motion to quash a subpoena that presents an unreasonable invasion of their customers' private records.[241] There is also a real risk that unsophisticated subpoena recipients will not know of their right to challenge such a demand.[242] Further, since the subpoena would come directly from the FBI, and could come with an order of secrecy, some recipients likely will be intimidated into complying with even unreasonable demands for fear of negative repercussions.[243] As a consequence, the administrative subpoenas would not substitute probable cause with a lower standard of scrutiny under the Fourth Amendment: instead, they would substitute probable cause for no review at all, effectively granting the FBI non-reviewable demand power to obtain private information on which to base a criminal prosecution. For both search warrants and administrative subpoenas, review by a neutral judicial body legitimizes the state's invasion of individuals' privacy.[244] Congress cannot justify the use of administrative subpoenas for terrorism investigations merely with talk of the safeguard created by judicial review,[245] because, in this context, no neutral body would protect subpoena recipients from agency overreaching. If the FBI were armed with administrative subpoena power, judicial review would not guard individuals swept up in a terrorism investigation from unreasonably intrusive demands.

---

237. *See* Doe v. United States, 253 F.3d 256 (4th Cir. 2001); United States v. Bailey, 228 F.3d 341 (6th Cir. 2000).

238. *Doe*, 253 F.3d at 256; *Bailey*, 228 F.3d at 341.

239. *See* S. 2555, 108th Cong. (2004); H.R. 3037, 108th Cong. (2003); *supra* Introduction.

240. *See* S. 2555; H.R. 3037.

241. *See* Unchecked Power, *supra* note 178; *supra* notes 174-84 and accompanying text.

242. *See supra* notes 185-86 and accompanying text.

243. *See* Bantam Books, Inc. v. Sullivan, 372 U.S. 58, 68-70 (1963); *supra* notes 188-90 and accompanying text.

244. *See supra* notes 25-27, 90-98 and accompanying text.

245. For an example of this justification, see Brand Testimony, *supra* note 158.

Second, since administrative subpoenas will likely be used for data mining, mission creep could further undermine Fourth Amendment rights. Unlike information subpoenaed by a grand jury, information obtained through administrative subpoenas is not subject to exacting use restrictions.[246] Even if Congress could justify abrogating Fourth Amendment rights for the needs of terrorism investigators, data mining conducted on the data sets retrieved by administrative subpoenas will likely reveal other criminal activity unrelated to terrorism.[247] For example, if the agents in the hypothetical above[248] did obtain the sales records of every hardware store in a regional area and searched through those records for evidence of suspicious activity, criminal activity wholly unrelated to terrorism, such as credit card fraud, could surface. If the government used this evidence to prosecute individuals for other, non-terrorism related crimes, the Fourth Amendment policies effectuated by the probable cause requirement would be further subverted. Mission creep would tacitly enable the FBI to circumvent the probable cause requirement in criminal investigations beyond terrorism investigations.[249]

C. *Recommendation for Congress*

Identifying the necessary and best tools to fight terrorism is far beyond the scope of this Note. The decision to abrogate Fourth Amendment privacy rights for the benefit of terrorism investigations is a choice that Congress must consider, and the federal courts will assess, in light of the circumstances. If Congress does grant the FBI administrative subpoena power for terrorism investigations, Congress must provide strong justifications for seriously compromising the Fourth Amendment rights of all individuals caught up in these investigations. However, in the alternative, Congress should also act decisively to prevent the damage to Fourth Amendment rights from spreading beyond the context of terrorism investigations. Specifically:

(1) Congress should prevent mission creep by placing limits on the future use of any information obtained with administrative subpoenas in a non-terrorism context. This could be accomplished by placing statutory limits on the future use of any database created from subpoenaed information for a non-terrorism criminal investigation. The restrictions need not be as strict as grand jury secrecy

246. *See supra* notes 104-05 and accompanying text. Although grand jury subpoenas could give investigators access to similar quantities of private information without probable cause, the Federal Rules of Criminal Procedure strictly limit the use of that information. Fed. R. Crim. P. 6(e); *see supra* notes 55-63 and accompanying text.

247. *See* DeRosa, *supra* note 198, at 16; Seifert, *supra* note 209, at 12-13; Schulhofer, *supra* note 215, at 85; *supra* notes 211-15 and accompanying text.

248. *See supra* Introduction.

249. *See supra* note 215 and accompanying text.

requirements;[250] the statutory provision could parallel the provision in HIPAA[251] that has successfully protected patients' private information from use in non-health care fraud investigations.[252] Congress could also require regular reporting by the Attorney General on the measures taken to prevent misuse of the database. As in the health care fraud context, this will keep the probable cause requirement intact in other investigations where the reasonableness standard remains inappropriate.[253]

(2) Congress should explicitly confine any administrative subpoena issuing power to as few persons as possible. In the terrorism context, the subpoenas will not be subject to neutral review for reasonableness.[254] However, if agents directly involved in an investigation must seek review from outside their own agency, albeit in another executive department, review by a party removed from the investigation would subject the subpoenas' reasonableness to questioning by a more neutral party. Although this informal check would not provide the same balance as review by neutral judicial officers, at the very least such informal gatekeeping power and prosecutors' asymmetrical accountability could prevent blatantly unreasonable agency demands and extreme cases of agency overreaching.[255]

These suggestions place only mild checks on administrative subpoena power and would not protect the privacy rights of terrorism administrative subpoena recipients. However, these checks will prevent the further erosion of Fourth Amendment rights in non-terrorism contexts absent public debate. Even if Congress can justify abrogating Fourth Amendment privacy rights for terrorism investigations, these checks would uphold Fourth Amendment policies in other criminal investigations.

CONCLUSION

By giving administrative subpoena power to prosecutors for health care fraud cases under HIPAA, Congress sanctioned the use of civil Fourth Amendment standards in criminal investigations and subsequent prosecutions.[256] Given the Department of Justice's success with administrative subpoenas in the health care fraud context, granting administrative subpoena power to terrorism

250. *See* Fed. R. Crim. P. 6(e).
251. 18 U.S.C. § 3486(e) (2000).
252. *See* DOJ Report, *supra* note 6, at 35.
253. *See supra* Part I.C.3.
254. *See supra* Part II.A.2.
255. *See supra* Part I.C.4.
256. *See* Doe v. United States, 253 F.3d 256, 263-64 (6th Cir. 2001); United States v. Bailey, 228 F.3d 341, 346-47 (4th Cir. 2000); *supra* notes 118-31 and accompanying text.

investigators could be an effective way to help prevent a crime with infinitely high social costs.[257] However, because health care fraud investigations are not analogous to terrorism investigations, Congress should not give the FBI additional administrative subpoena power without compelling reasons for abrogating long-standing principles of Fourth Amendment rights. Even if Congress could justify granting administrative subpoena power to the FBI for terrorism investigations, Congress must still take additional action to ensure that Fourth Amendment rights in other criminal investigations are not similarly undermined.

257. *See* 150 Cong. Rec. S7179-80 (daily ed. June 22, 2004) (statement of Sen. Kyl explaining the provisions of S. 2555); Updating the Law, *supra* note 7; *supra* notes 144-52 and accompanying text.